



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

Address: COMMISSIONER FOR PATENTS

P.O. Box 1450

Alexandria, Virginia 22313-1450

www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/675,491

09/30/2003

Jeyhan Karaoguz

14822US02

6014

23446

7590

08/26/2008

MCANDREWS HELD & MALLOY, LTD

500 WEST MADISON STREET

SUITE 3400

CHICAGO, IL 60661

EXAMINER

RYAN, PATRICK A

ART UNIT

PAPER NUMBER

2623

MAIL DATE

DELIVERY MODE

08/26/2008

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

10/675,491

Applicant(s)

KARAOGUZ ET AL.

Examiner

PATRICK A. RYAN

Art Unit

2623

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 21 May 2008.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-26 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-26 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-946)
- 3) ☐ Information Disclosure Statement(s) (PTO/SI/309)
Paper No(s)/Mail Date _____
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date _____
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: _____

DETAILED ACTION

1. This Office Action is made in response to Amendment-After Non-Final Rejection ("Reply") filed May 21, 2008. Applicant has amended Claims 1-5, 7-15, 18-19, 21, 23-24, and 26; no claims have been added; and no claims have been canceled. As amended, Claims 1 through 26 are presented for examination.
2. Applicant has amended the Specification Page 2 in order to provide the US Provisional Application Serial Numbers corresponding to the previously listed Attorney Docket Numbers.

Priority

3. Applicant claims priority to and benefit of the following US Provisional Applications: (60/432,472), filed December 11, 2002; (60/443,894), filed January 30, 2003; (60/457,179), filed March 25, 2003; (60/461,717), filed April 10, 2003; and (60/464,697), filed April 23, 2003.
4. The Examiner has found support for the claims of the instant application in:

(60/457,179), titled "Server Architecture Supporting a Personal Media Exchange Network" (for example Fig. 2 supported by Paragraphs [58-66] describing the process of registering and establishing user connections on a media exchange network).

(60/461,717), titled "Secure Media Peripheral Association with Authentication in a Media Exchange Network" (for example Fig. 2B showing a method of authentication of user equipment using a certificate key, as described in Paragraph [49-52]).

(60/464,697), titled "Secure Linking with Authentication and Authorization in a Media Exchange Network" (for example Fig. 2A showing a method of user authentication and confirmation of a user's digital certificate information, as described in Paragraphs [36-46]).

5. The Examiner does not find support for the claims of the instant application in:

(60/432,472), titled "Personal Inter-Home Media Exchange Network" (Paragraphs [17, 23, 29, 30, 36, and 37] mention "authentication", "authorization", and "digital certificate"; but these paragraphs and the included figures do not support a method of or system for authenticating or authorizing a user on a media exchange network. The document is primarily related to the sharing and accessing media on a media exchange network, with reference to Paragraphs [01-06] and Fig. 5).

(60/443894), titled "Access and Control of Media Peripherals via a Media Processing System" (Paragraphs [73, 90, and 91] mention authorization as a client function, but the document is primarily directed toward controlling media peripheral devices and providing a user friendly interface for interacting with the media peripheral devices on the media exchange network, with reference to Paragraphs [05-15] and Fig. 2A-2B).

6. It is therefore the Examiner's position that the Applicant's earliest supported claim of priority is to Provisional Application (60/457,179) filed March 25, 2003.

Response to Arguments

7. Applicant's arguments with respect to claims 1 through 26 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

9. Claims 1-12, 14, and 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ellis et al., United States Patent (6,774,926 B1), hereinafter "Ellis", in view of Takanashi et al., United States Patent Application Publication (2003/0177249 A1), hereinafter "Takanashi".

10. In regards to Claim 1, Ellis teaches a method for establishing a communication pathway for subsequent media exchanges between a television display in a first home and storage that contains media in a second home (As shown Figs. 1 and 7, multiple User Equipment, such as Contributor 102 and Viewer 104, interact over Communications Network 106. Furthermore, Contributor 102 can have storage equipment that viewers on the network, such as Viewer 104, can access and use to retrieve programs, as described in Col. 10 Lines 17-33. User Equipment can be based on a set-top box, a television, or a computer, as described in Col. 1 Lines 46-56. In addition, each of Contributor 102 and Viewer 104 can be required to enter a password,

Option 200 and Option 213 of Fig. 14, in order to modify stored content or gain access to stored content, as described in Col. 11 Line 53—Col. 12 Line 16).

Ellis does not teach securely transferring authorization and addressing information between a television in a first home and a storage in a second home or requesting confirmation of the security information.

In a similar field of invention, Takanashi teaches a method and system for limiting unauthorized access to a network. Takanashi creates and transmits an address correlation to a client using the method of Fig. 6 for assigning Internet Protocol (IP) address to each client on the system, as described in Paragraph [0034-0035]. In addition, Takanashi requires each client to enter a User ID and password, which is compared to data stored in User Database 130, to determine the validity of the data provided by the user. A client is provided access to Network 110 once an IP address has been assigned and the User ID and password are judged to be correct ("Affirmative Confirmation"), as described in Paragraphs [0022-0024, 0027-0031]; with further reference to Figs. 6 and 7, as described in Paragraphs [0034-0037]. The User ID and password allow the authorization and addressing information to be securely transferred to the user. In addition, IP Assignment System 125 forwards the IP address, leasing time, and renewal window data to the client in a DHCP reply packet ("Storing Affirmative Confirmation"), as Takanashi discloses in Paragraph [0022].

It would have been obvious to one of ordinary skill in the art at the time of the invention to combined the method of providing a communications channel between users on a network using a central server, which is accessed by password, as taught by

Ellis; with the method of assigning an IP address to a client and storing an association of the IP address with client data (such as a User ID and password) in a DHCP packet, as taught by Takanashi, in order to reduce the chances of unauthorized access to the network, such as by a hacker (as Takanashi discusses in Paragraphs [0003-0010]).

11. In regards to Claim 2, the combination of Ellis and Takanashi teach the method according to Claim 1, comprising associated with the subsequent media exchanges, verifying that the affirmative confirmation has been stored (DHCP reply packet of Takanashi includes a leasing time and renewal window, as described in Paragraph [0022]. Based on the renewal window, the client system must return a renewal packet to Access System 145 in order to continue affirmative confirmation of the assigned IP address, as Takanashi teaches in Paragraphs [0023]; with further reference to Figs. 6 and 7, as described in Paragraph [0034-0037]).

12. In regards to Claim 3, the combination of Ellis and Takanashi teach the method according to Claim 2, comprising receiving one or both of the address correlation information associated with the television display in the first home and/or the address correlation information associated with the storage in the second home via at one or both of an in-band channel and/or an out-of-band channel (Takanashi teaches receiving address correlation information, as addresses regarding Claims 1 and 2, and Ellis teaches the communication of information using an out-of-band channel, as described in Col. 4 Lines 42-53).

13. In regards to Claim 4, the combination of Ellis and Takanashi teach the method according to Claim 1, wherein one or both of the address correlation information

associated with the television display in the first home and the address correlation information associated with the storage in the second home is one or more of a digital certificate, a one-time digital certificate, a one-time code, a device identification, and/or a key (Takanashi teaches address correlation information in the form of IP address assignments, as described in Paragraphs [0022-0023, and 0034]; with further reference to Fig. 6).

14. In regards to Claim 5, the combination of Ellis and Takanashi teach the method according to Claim 1, further comprising limiting a period for which one or both of the address correlation information associated with the television display in the first home and/or the address correlation information associated with the storage in the second home is valid (Takanashi teaches the use of leasing and renewal time, which limits the window of time in which an IP address assigned to a client is valid, as described in Paragraphs [0032-0033, and 0036-0037]; with further reference to Figs. 5A, 5B, and 7).

15. In regards to Claim 6, Ellis teaches a method for establishing a communication pathway for subsequent media exchange between a first media component in a first home and a second media component in a second home (As shown Figs. 1 and 7, multiple User Equipment, such as Contributor 102 and Viewer 104, interact over Communications Network 106. Furthermore, Contributor 102 can have storage equipment that viewers on the network, such as Viewer 104, can access and use to retrieve programs, as described in Col. 10 Lines 17-33. User Equipment can be based on a set-top box, a television, or a computer, as described in Col. 1 Lines 46-56. In

addition, each of Contributor 102 and Viewer 104 can be required to enter a password, Option 200 and Option 213 of Fig. 14, in order to modify stored content or gain access to stored content, as described in Col. 11 Line 53—Col. 12 Line 16).

Ellis does not teach transferring authorization and addressing information between a media component in a first home and a media component in a second home or requesting confirmation of the information.

In a similar field of invention, Takanashi teaches a method and system for limiting unauthorized access to a network. Takanashi creates and transmits an address correlation to a client using the method of Fig. 6 for assigning Internet Protocol (IP) address to each client on the system, as described in Paragraph [0034-0035]. In addition, Takanashi requires each client to enter a User ID and password, which is compared to data stored in User Database 130, to determine the validity of the data provided by the user. A client is provided access to Network 110 once an IP address has been assigned and the User ID and password are judged to be correct ("Affirmative Confirmation"), as described in Paragraphs [0022-0024, 0027-0031]; with further reference to Figs. 6 and 7, as described in Paragraphs [0034-0037].

It would have been obvious to one of ordinary skill in the art at the time of the invention to combined the method of providing a communications channel between users on a network using a central server, which is accessed by password, as taught by Ellis; with the method of assigning an IP address to a client and storing an association of the IP address with client data (such as a User ID and password) in a DHCP packet,

as taught by Takanashi, in order to reduce the chances of unauthorized access to the network, such as by a hacker (as Takanashi discusses in Paragraphs [0003-0010]).

16. In regards to Claim 7, the combination of Ellis and Takanashi teach the method according to Claim 6, comprising storing the confirmation (IP Assignment System 125 forwards the IP address, leasing time, and renewal window data to the client in a DHCP reply packet, as Takanashi discloses in Paragraph [0022]).

17. In regards to Claim 8, the combination of Ellis and Takanashi teach the method according to Claim 7, comprising associated with the subsequent media exchange, verifying that the confirmation has been stored (DHCP reply packet of Takanashi includes a leasing time and renewal window, as described in Paragraph [0022]. Based on the renewal window, the client system must return a renewal packet to Access System 145 in order to continue affirmative confirmation of the assigned IP address, as Takanashi teaches in Paragraphs [0023]; with further reference to Figs. 6 and 7, as described in Paragraph [0034-0037]).

18. In regards to Claim 9, the combination of Ellis and Takanashi teach the method according to Claim 6, comprising receiving one or more of the address correlation information in the first home, the address correlation information in the second home and/or the routing address via one or both of an in-band channel and/or an out-of-band channel (Takanashi teaches receiving address correlation information, as addresses regarding Claims 1 and 2, and Ellis teaches the communication of information using an out-of-band channel, as described in Col. 4 Lines 42-53).

19. In regards to Claim 10, the combination of Ellis and Takanashi teach the method according to Claim 6, wherein one or both of the address correlation information in the first home and/or the address correlation information in the second home is one or more of a digital certificate, a one-time digital certificate, a one-time code, a device identification and/or a key (Takanashi teaches address correlation information in the form of IP address assignments, as described in Paragraphs [0022-0023, and 0034]; with further reference to Fig. 6).

20. In regards to Claim 11, the combination of Ellis and Takanashi teach the method according to Claim 6, further comprising limiting a period for which one or both of the address correlation information in the first home and the address correlation information in the second home is valid (Takanashi teaches the use of leasing and renewal time, which limits the window of time in which an IP address assigned to a client is valid, as described in Paragraphs [0032-0033, and 0036-0037]; with further reference to Figs. 5A, 5B, and 7).

21. In regards to Claim 12, Ellis teaches a system that supports media exchange between a first home and a second home, system comprising: a television display in the first home and storage that contains media in a second home (Personal Television Program System 30 of Fig. 1; with further reference to Fig. 7 showing a Contributor at User Equipment 102 and a Viewer at User Equipment 104, as described in Col. 7 Line 27-Col. 8 Line 16. User Equipment can be based on a set-top box, a television, or a computer, as described in Col. 1 Lines 46-56. In addition, each of Contributor 102 and

Viewer 104 can be required to enter a password, Option 200 and Option 213 of Fig. 14, in order to modify stored content or gain access to stored content, as described in Col. 11 Line 53—Col. 12 Line 16).

Ellis does not teach transferring authorization and addressing information between a television display in a first home and a storage in a second home or requesting confirmation of the information by way of a secure server.

In a similar field of invention, Takanashi teaches a method and system for limiting unauthorized access to a network. Takanashi creates and transmits an address correlation to a client using the method of Fig. 6 for assigning Internet Protocol (IP) address to each client on the system, as described in Paragraph [0034-0035]. In addition, Takanashi requires each client to enter a User ID and password, which is compared to data stored in User Database 130, to determine the validity of the data provided by the user. A client is provided access to Network 110 once an IP address has been assigned and the User ID and password are judged to be correct ("Affirmative Confirmation"), as described in Paragraphs [0022-0024, 0027-0031]; with further reference to Figs. 6 and 7, as described in Paragraphs [0034-0037]. In addition, Access Control Server 140, shown in Fig. 1 and further detailed in Fig. 4, is used to validate the client's User ID and password, and control a client's access to Network 110, as described in Paragraph [0031].

It would have been obvious to one of ordinary skill in the art at the time of the invention to combined the system for providing a communications channel between users on a network using a central server, which is accessed by password, as taught by

Ellis; with the system for assigning an IP address to a client and storing an association of the IP address with client data (such as a User ID and password) in a DHCP packet, as taught by Takanashi, in order to reduce the chances of unauthorized access to the network, such as by a hacker (as Takanashi discusses in Paragraphs [0003-0010]).

22. In regards to Claim 14, the combination of Ellis and Takanashi teach the system according to Claim 12, wherein the one or both of the first routing address and/or the second routing address is communicated via at one or both of an in-band channel and/or an out-of-band channel (Takanashi teaches receiving address correlation information, as addresses regarding Claims 1 and 2, and Ellis teaches the communication of information using an out-of-band channel, as described in Col. 4 Lines 42-53).

23. In regards to Claim 15, the combination of Ellis and Takanashi teach the system according to Claim 12, wherein the server authenticates an initial access of one or both of the television display having an associated first routing address and/or the storage having an associated second routing address (Takanashi teaches Access System 145 of Access Control Server 140 that verifies a clients User ID and password before assigning the client an IP address, as described in Paragraph [0036]).

24. Claim 13 is rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Ellis and Takanashi as applied to Claim 15 above, and further in view of Humpleman et al., United States Patent (6,182,094 B1).

25. In regards to Claim 13, the combination of Ellis and Takanashi teach the system according to Claim 12. In addition, Takanashi teaches that DHCP server 120 assigns P address to clients on the network and can reallocate the IP address if the IP assignment is cancelled (as discussed in Paragraph [0007]). Takanashi's disclosure suggests, but does not explicitly teach that the server comprises a memory that stores one or both of the first routing address and/or the second routing address.

In a similar field of invention, Humpleman teaches a method and system using a DHCP server (106/306) that acts as a configurations manager for Home Network 100, with reference to Figs. 1 and 4A. In addition, Humpleman teaches that DHCP Server stores the generated IP addresses and logical name pair within a device list, as described in Col. 11 Lines 35-55 and Col. 12 Lines 12-21.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the system of providing a secure communications channel in a media exchange network, as taught by the combination of Ellis and Takanashi to include a DHCP server that stores the IP addresses of clients on the network, as taught by Humpleman, in order to have a centrally stored record of all devices on the network and a record of IP addresses that have been assigned and that are available.

26. Claims 16-18, and 20-26 rejected under 35 U.S.C. 103(a) as being unpatentable over Ellis in view of Yoon et al., United States Patent Application Publication (2002/0004832 A1), hereinafter "Yoon".

27. In regards to Claim 16, Ellis teaches a system for communicating information (Personal Television Program System 30 of Fig. 1; with further reference to Fig. 7), the system comprising: a first device (Data Storage Facility 52 of Fig. 1 that hosts an interface for allowing a contributor of media and a viewer of media to enter a password in order to gain access to the communications network, as described in Col. 11 Line 53 - Col. 12 Line 16. In addition, the operations of Data Storage Facility 52 can be performed by one or more servers, such as Servers 112, 116, or 118 or Fig. 7, as described in Col. 4 Lines 59-67), a second device (Viewer at User Equipment 104 of Fig. 7, as described in Col. 7 Line 27-Col. 8 Line 16), and a third device (Contributor at User Equipment 102). In addition, Ellis teaches that Contributor at User Equipment 102 transfers media to the Viewer at User Equipment 104, as described in Col. 3 Line 55 - Col. 4 Line 5.

Ellis does not teach a processor used to issue access information to a second and third device by way of a first device or that the processor authenticates access information between the second and third devices.

In a similar field of invention, Yoon teaches a system and method for establishing a communications channel between a Local Computer 30 and an Internet Server 60 (Abstract, with further reference to Figs. 1 and 4). Yoon also teaches the communicating and assigning access information in the form of a Temporary ID and Password that is assigned based on the confirmation of a requester's IP address. In addition, Yoon teaches a processor, Connection Authentication Server 50, which communicates access information between the Local Computer 30 and the Internet

Server 60, as described in Paragraphs [0030-0032]. The Connection Authentication Server 50 transfers access information to the Local Computer 30 through the process of Steps 100 and 102 ["from first to third device" where the processor resides at the first device]. In addition, the Connection Authentication Server 50 issues this access information to the Internet Server 60 is Step 104 of Fig. 4 ["first to second device"]. Yoon also teaches that Local Computer 30 request connection authentication in Step 100 before requesting the services of Internet Server 60 ["authenticates the access information"] (as described in Paragraphs [0038-0039], with reference to Fig. 4; with further reference to Step 314 of Fig. 6, as described in Paragraph [0060-0061]).

Both Ellis and Yoon teach communication systems in which a secure communications pathway is established between devices on a network. In addition, both Ellis and Yoon utilize a server to authenticate the devices that request access to the network. Ellis teaches requiring each user on the network to enter a password in order to gain access and transfer media by way of a central server (using Data Storage Facility 52). Yoon teaches authenticating a user's IP address and then issuing a Temporary IP and Password so that the user can access the network (using Connection Authentication Server 50). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the system for providing a communications channel between users on a network, which is accessed by password, as taught by Ellis, to include the Connection Authentication Server taught by Yoon in order to enhance the security of the system (as Yoon describes in Paragraph [0013]).

28. In regards to Claim 17, the combination of Ellis and Yoon teach the system according to Claim 16, wherein the at least one processor communicates the access information from the at least the second device to the third device (Yoon teaches the transmission of Connection Admission Signal 108 from Internet Server 60 to Local Computer 30, as shown in Fig. 4 and described in Paragraphs [0038-0039]).

29. In regards to Claim 18, the combination of Ellis and Yoon teach the system according to Claim 17, wherein the at least one processor communicates the access information from the at least the second device to the third device via one or both of an in-band channel and/or an out-of-band channel (Ellis teaches the communication of information using an out-of-band channel, as described in Col. 4 Lines 42-53).

30. In regards to Claim 20, the combination of Ellis and Yoon teach the system according to Claim 16, wherein the first device is a media exchange server (Ellis teaches Data Storage Facility 52 of Fig. 1 as described in Col. 4 Lines 42-67; with further reference to Fig. 7).

31. In regards to Claim 21, the combination of Ellis and Yoon teach the system according to Claim 16, wherein the at least the second device and the third device is one or more of a media processing system, a personal computer executing media exchange software, and a media peripheral (Ellis teaches User Equipment 102 and 104, which can be based on a set-top box, a television, or a computer, as described in Col. 1 Lines 46-56).

32. In regards to Claim 22, the combination of Ellis and Yoon teach the system according to Claim 16, wherein the at least one processor permits the third device to

communicate with the at least the second device, if the access information is authenticated by the first device (Authentication Server 50 determines the authenticity of the IP address "N" received from Local Computer 30, as shown in Step 306 of Fig. 6 and described in Paragraphs [0052-0055]. If Local Computer 30 is authenticated, a Temporary ID and Password are generated at Step 314, which are used to open the communications channel as show in Step 110 of Fig. 4, as described in Paragraph [0039]).

33. In regards to Claim 23, the combination of Ellis and Yoon teach the system according to Claim 16, wherein the at least one processor one or both of denies and/or restricts the transfer of the at least one of media, data, and, service between the at least the second device, if the access information is not authenticated by the first device (Authentication Server 50 determines the authenticity of the IP address "N" received from Local Computer 30, as shown in Step 306 of Fig. 6 and described in Paragraphs [0052-0055]. If Local Computer 30 is not authenticated then Step 318 is executed where a refusal signal is transmitted, which denies Local Computer 30 access to the network, as described in Paragraph [0055]).

34. In regards to Claim 24, the combination of Ellis and Yoon teach the system according to Claim 16, wherein the access information is one or more of a digital certificate, a one-time digital certificate, a one-time code, a device identification and/or a key (Yoon teaches a Temporary ID and Password that is assigned based on the confirmation of a requester's device identification in the form of an IP address, as described in Paragraph [0038]).

35. In regards to Claim 25, the combination of Ellis and Yoon teach the system according to Claim 16, wherein the at least one processor limits a period for which the access information is valid (Yoon teaches Authentication Server 50 can assign an Authentication Time "T" to the Temporary ID and Password, as disclosed in Paragraph [0058]; with further reference to Step 408 of Fig. 7, as described in Paragraph [0068]).

36. In regards to Claim 26, the combination of Ellis and Yoon teach the system according to Claim 16, wherein the at least one processor is one or more of a computer processor, a media peripheral processor, a media exchange system processor, a media exchange server processor and/or a media processing system processor (Ellis teaches a media exchange system processor shown as Data Storage Facility 52 of Fig. 1 and described in Col. 4 Lines 42-67; with further reference to Fig. 7).

37. Claim 19 is rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Ellis and Yoon as applied to Claim 17 above, and further in view of Woodhill, United States Patent (6,934,858 B2).

38. In regards to Claim 19, the combination of Ellis and Yoon teach the system according to Claim 17, but the combination does not teach system comprising a telephone device that is utilized to inform a user of the third device of the access information.

39. In a similar field of invention, Woodhill teaches a method and system for authenticating and authorizing a user wishing to participate in an electronic transaction

on a communications network (Abstract, with further reference to Fig. 1). Woodhill teaches the use of Public Switched Telephone Network 44 and Telephone 46 in order to provide a user with confirmation information. This confirmation information is used to authenticate the user by way of Authentication/Authorization Service 38 for access to Target Site 30 (as shown in Fig. 1 and described in Col. 8 Lines 12 – Col. 9 Line 5). 40. It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the system for establishing a communications channel between authorized devices on a network, as taught by the combination of Ellis and Yoon, to include a telephone device to inform a user of access information, as taught by Woodhill, in order to provide a real-time and secure means of authenticating a user (as Woodhill describes Col. 5 Line 24 - Col. 6 Line 23; with further reference to Table II in Col. 5).

Conclusion

41. Any inquiry concerning this communication or earlier communications from the examiner should be directed to PATRICK A. RYAN whose telephone number is (571)270-5086. The examiner can normally be reached on Mon to Thur, 8:00am - 5:00pm EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Scott Beliveau can be reached on (571) 272-7343. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/P. A. R./
Examiner, Art Unit 2623
Monday, August 25, 2008

/Scott Beliveau/
Supervisory Patent Examiner, Art Unit 2623